HOW SYSTEMS ENGINEERING AND RISK MANAGEMENT DEFEND AGAINST MURPHY'S LAW AND HUMAN ERROR

Michael Bay
Jackson and Tull, Aerospace Engineering Division
michael.bay@gsfc.nasa.gov

Warren Connley
NASA Goddard Spaceflight Center
warren.e.connley@nasa.gov

Abstract

Systems Engineering and Risk Management processes can work synergistically to defend against the causes of many mission ending failures. Defending against mission ending failures is facilitated by fostering a team that has a healthy respect for Murphy's Law and a team with a sense of curiosity for how things should work, how they can fail, and what they need to know.

This curiosity is channeled into making the unknowns known or what is uncertain more certain. Efforts to assure mission success require the expenditure of energy in the following areas:

1. *Understanding what defines Mission Success as guided by the customer's needs, objectives and constraints.*
2. *Understanding how the system is supposed to work and how the system is to be produced, fueled by the curiosity of how the system should work and how it should be produced.*
3. *Understanding how the system can fail and how the system might not be produced on time and within cost, fueled by the curiosity of how the system might fail and how production might be difficult.*
4. *Understanding what we need to know and what we need learn for proper completion of the above three items, fueled by the curiosity of what we might not know in order to make the best decisions.*

The challenge behind the "management" part of risk management (or systems management and project management), is to identify what is important for achieving mission success and then deciding to apply resources where they will do the most good.

Another challenge is keeping curiosity alive to prevent complacency and a sense of infallibility from interfering with team members asking important "What can go wrong" type questions. Threats to mission success are attitudes exemplified by responses such as "It has never failed before," or "We have never done this before" when given to resource allocation questions.

Successful teams place value in reliable hardware, they know that it takes rigor and discipline to achieve mission success and they expend energy to achieve it. These teams also stick to tried and proven values and principles that form the foundation of mission success. They are not easily swayed by new "fads" or external pressure to change.

Successful teams also understand that "Risk Management" is not a separate disciple from Engineering, Mission Assurance or Project Management. Risk management is a technique performed by everyone and should not be left to "outside analysts" who are called on to "save" the team from making mistakes or make up for lapses in engineering and management.

Murphy's Law

Murphy's Law states "Anything that can go wrong will go wrong." Restated a bit differently, when an unrecognized flaw exists, if the seeds for a problem have been sewn, then it is almost certain to manifest itself into a problem or failure if and when the proper initiating conditions arise. This is quite evident from the failure history of space missions. Many if not all elements have to

work properly and it only takes one latent defect or malfunction to cause a serious problem.

Figure 1 illustrates a natural tension between Murphy's Law and Mission Success. This diagram is used to illustrate 1) that one of many common causes of flight failures can result in a "weak link" of the system, you have to watch out for all of them, 2) that most causes are human error related, and 3) can be mitigated by a multilayered defense.[1]

Murphy's law is a practical consequence of the second law of thermodynamics which states that energy concentrated in an ordered fashion naturally dissipates to a more distributed and disordered state. It takes energy to keep systems operating properly and energy to stay on top of all the details inherent in complex aerospace systems.

Like wise project teams developing complex systems have to expend energy and resources to keep rigor and discipline in place and prevent complacency from interfering with an appropriate focus on sound risk management and systems engineering principles.

Mission ending failures are generally not random. They are introduced by a mistake, an error, a decision, or an assumption that is not correct, in other words human error.[2] Mission ending flaws are usually not the result of "random parts failures" as predicted by classical MIL-STD-217 or similar reliability predictions. Most mission ending flaws are due to preventable errors. They are preventable because if the flaw's existence had been "known" they would have been caught and corrected. This is opposed to an "unknowable" random parts failure or an unknown consequence of a new technology. If flaws exist then it is almost certain to surface as a problem when the initiating conditions arise or line up. Risk Management seeks to make these "knowable unknowns" known so they can be mitigated before they turn into a problem.

For any given system there is a probability that a mission ending flaw exists. This probability is inversely related to the energy, rigor and discipline applied to the defenses designed to protect the system against human error. It is unreasonable to require or expect a single person to complete a mission critical task flawlessly. So we assemble project teams and organizations that work together, check each other's work, and back each other up in order to identify and correct flaws. Teams expend energy to find these flaws before they turn into problems. Success in complex aerospace systems is based on

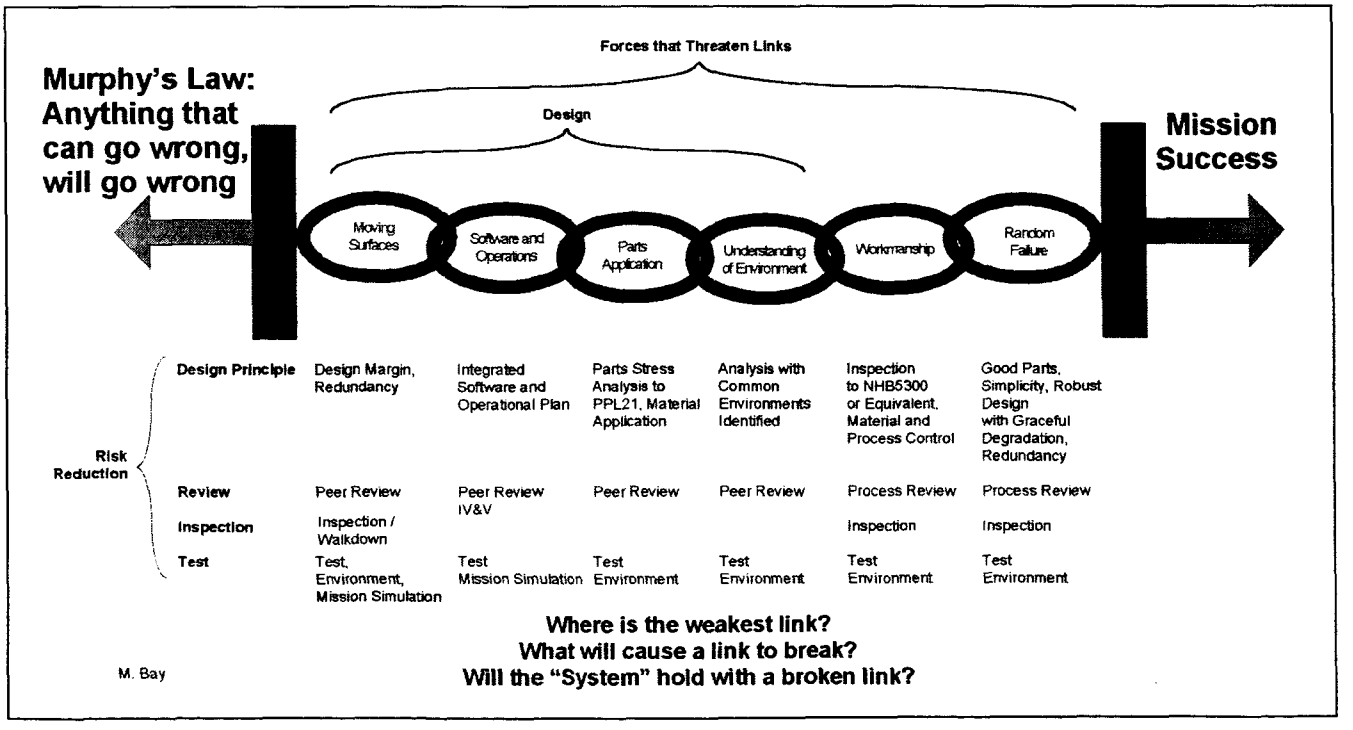

Figure 1 System Weak Links

multilayer defenses or a defense in the collective depth of the team.

Successful teams have a respect and skepticism that borders on a preoccupation with potential failures. They exhibit a continued and constant concern for failures by expending energy and resources in order to find latent flaws.

Defending against uncertain events with uncertain outcomes is sometimes difficult especially for those who have not experienced failures. Asking the right kind of risk management questions can be difficult for those without experience. Experience lets you get ahead of the power curve and anticipate what could go wrong.[3] While it is hard to replace experience, there are sources of information that must be sought out to avoid repeating mistakes and lessons already learned in the past.

Deciding to expend energy and resources for risk management can be a difficult decision especially when the benefit or positive result is not immediately visible. Results may never be visible, after all when the mission is successful, is it because of good risk management or sound engineering? A resource constrained climate, that repeatedly asks "Why is this effort necessary?", can also stifle the effort necessary for good risk management. Successful teams know where resources are needed and will go fight for them.

Teams need to constantly expend energy, they need to be vigilant and work with discipline and rigor to identify and correct potential problems and flaws before they surface and cause problems. This energy must not only go into the technical effort but also into the guidance of the processes that defines and guides the technical work.

It is Risk Management's function to seek out those things that we do not yet know and make them known, to identify where potential problems or flaws might exist and to accept the risk or apply resources to either identify and correct the flaw, alter the outcome, or reduce the likelihood of the outcome.

Conquering the Unknowns and Uncertainty

Once a "test" has passed and one has received some positive feedback that no problem has surfaced, there is a natural tendency and inclination in our human nature to gain confidence that one has conquered the unknown and therefore has reduced risk going forward. Once there has been a success, once the unknown has been conquered, we tend to move on to the next challenge. Without our ability to move on we would be paralyzed with a chicken little "The sky is falling" fear. However we need to be careful that we do not read too much into a success. We should not leave a conquered situation too soon, for the reality of the situation may change the next time.

For example, when faced with the decision whether to go ice skating on a pond, one recognizes that there is risk with skating on the ice. If the ice is too thin then one might fall through the ice and possibly drown. For a given location on the pond and a given time, nature and the laws of physics of the situation will determine the outcome. The reality of the situation is that either the ice is thick enough or it is not. The skater however does not know the reality of the situation. There is uncertainty in the mind of the skater. The uncertainty lies in the likelihood of an undesired consequence once proceeding onto the ice.

This uncertainty in the mind of the skater is felt or perceived as risk. Until the skater performs a test or receives direct or indirect evidence about the thickness of the ice, the risk may remain high. Once a test has been performed either by drilling a hole and measuring the thickness of the ice or by incrementally testing the strength of the ice in order to verify its ability to carry the weight of the skater, the skater will alter his perception of risk and proceed.

What some people forget is that performing the test did not actually change the real probability of falling through. Whether you fall through or not is set by physics and the laws of nature. Performing the test does however change the perceived likelihood of falling through. The test gives you an indication of margin. To change the

actual probability of falling through you need to change the physics of the situation like wearing shoes with a larger foot print to spread out the load. You can also change the consequence by putting on a life jacket and having a buddy with rescue equipment in order to alter the outcome of actually falling through.

A second misconception is that once a problem has been averted that the risk has been reduced going forward. Following up with the ice example, once the thickness has been confirmed it is assumed that the risk of falling through has been eliminated or reduced for the total surface area of the pond. This is not necessarily so. It is possible another area of the pond's iced surface might be thinner due to local heating by incoming ground water. Hopefully the skater considers this possibility while assessing the risks of skating on the pond from day to day. The skater should not assume the ice is safe today just because he did not fall through yesterday.

This is where margin helps. Margin is useful in providing a cushion between what is expected and what might be encountered unexpectedly. Continuing with the ice skating example, margin in the thickness of the ice is necessary to allow for unexpected events such as falling on the ice without cracking it and then falling through. There needs to be sufficient margin to account for the unknowns between what we think we know and nature's deterministic physics.

Questioning this natural optimistic tendency and remaining skeptical of test results requires energy. It is far easier to just accept success and

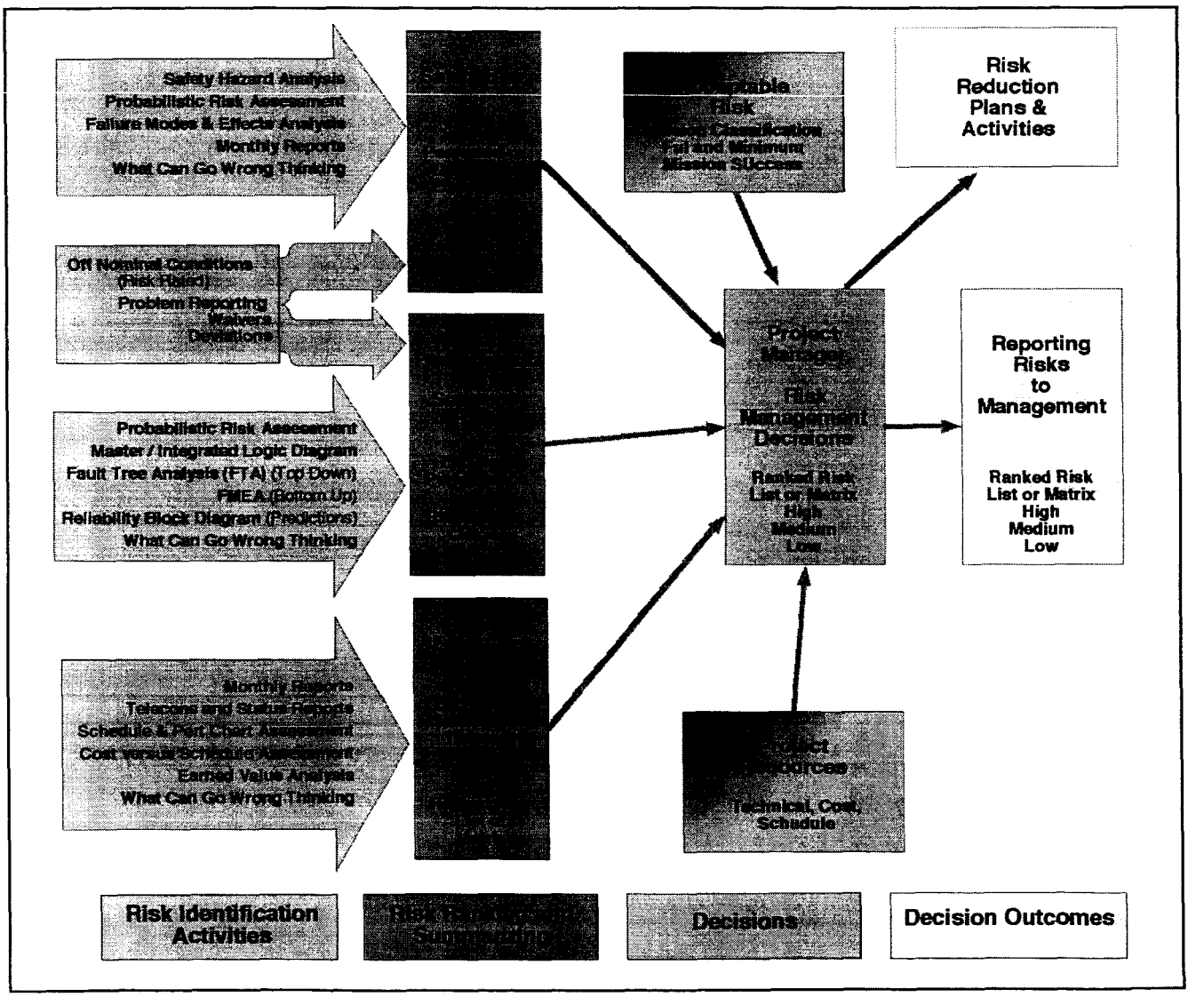

Figure 2 Risk Management Information Flow

think that the actual risk has reduced. If we do not remain vigilant that specific circumstances could be different as time passes or conditions change, what is not known or what is not asked could result in a problem.

Some seem to think that just because something has worked in a test or has flown before that there is no more risk. This is not true. They seem to think that a previous favorable result assures future success. A past success may have been a "random" success as opposed to the result of a rigorous, disciplined and repeatable process. A past success might also be due to a favorable stack up of conditions ending up with positive margin that will probably be different the next time. We need to expend energy fighting these misconceptions.

Galvanizing a Mission Success Orientated Team

Leaders "charge their team" with identifying risks to mission success. Leaders create an environment where curiosity (as mentioned above: a) for how things work, b) how they fail, and c) what they need to know) is encouraged. For the team to be effective their leaders must listen and understand any risks that are identified. In other words, leaders should not "shoot the messenger" when the risks arrive. The leader must be prepared to receive some risks that may not end up being significant risks worth mitigating but still require the expenditure of resources. Leaders should not fault or blame the risk identifier for having risks. If the leader does shoot the messenger, no further messages or risks will be brought to his attention

Leaders need to communicate to their teams that the purpose of identifying risks is to do something about them. Risks are brought to the leader's attention with the purpose of getting help with either technical, cost or schedule resources for mitigating risks or help with accepting the risks. If leaders do not help their teams with mitigating their risks, if there is little positive outcome of surfacing risks, then teams will not surface them, they will not get addressed or resolved resulting in real problems later on.

Figure 2 shows some basics elements of risk information flow. Risk information is identified, collected and reviewed against acceptable risk by Project Management who decide what technical, cost, and schedule resources if any are needed to lower the risk before it is accepted.

Leaders also need to expend energy to combat exaggerated senses of infallibility and/or complacency. Complacent responses to "What can go wrong questions" can range from, "Why worry, it has never failed before", "Better is the enemy of good enough", to "We have never done this before." These answers are <u>not</u> rooted in either sound risk management or engineering principles. A goal of leadership is to motivate the team to be curious about their system and to instill a skepticism that fights complacency.

<u>1. Understanding Mission Success.</u> In a global sense mission success can be viewed as safely collecting data or providing a service while completing it on time and within cost. Such a definition considers mission success from three perspectives; 1. Safety (bodily injury or facility damage), 2. Mission Performance (end item collecting data or providing a service), 3. Project Execution (delivering a quality product on time and within cost). This relationship is shown in Figure 3 as a three sided pyramid.[4]

The above mentioned view of mission success is consistent with NASA's "Mission Success Starts with Safety" policy while at the same time recognizes that the overall objective is to perform

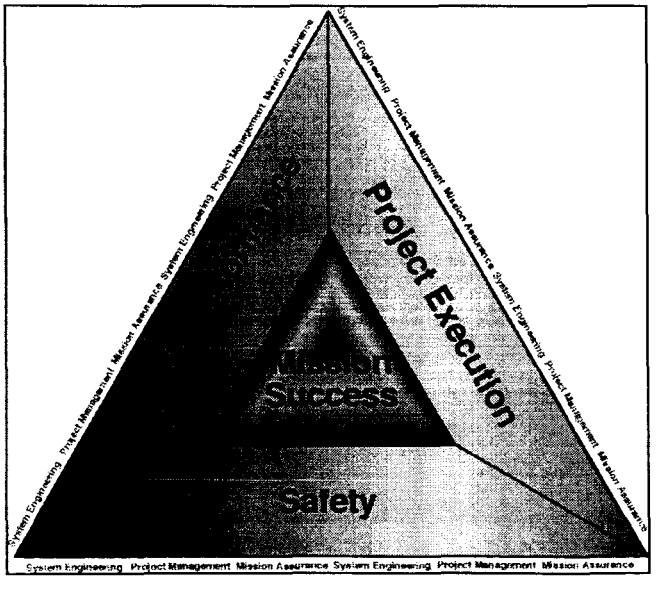

Figure 3 Mission Success Pyramid

a mission and execute the project within technical, cost, schedule, and risk constraints. Risk Management then seeks to reduce risks to mission success not as an isolated discipline but as a technique used by the team in order to achieve mission success in all three if these aspects.

Another reason for defining mission success from these three perspectives is that it helps guide risk management activities. If the goal of risk management is to reduce mission success risks, then these three aspects of mission success form three types of risk, Safety, Mission Performance, and Project Execution.

A key element of this distinction is that the techniques and skills necessary to identify these three risks types are different as are those who identify and accept the risks. Figure 2 identifies the different techniques for identifying each of the risk types.

The process for identifying the three types of risks is typically described in separate plans. Safety risk identification is described in a Safety Plan, Mission Performance Risk identification is described in a Reliability Program Plan, and Project Execution Risk identification is described in a Project Plan. The overall risk management process as shown in Figure 2 is document in a Risk Management Plan. In order for these plans to benefit the team the most they need to be generated for the specific project and describe exactly who will do what and when. It is the planning process that is important, as Dwight Eisenhower said, "Plans are nothing – planning is everything."

The team needs to understand mission success from the customer's viewpoint considering their needs, objectives, and constraints. Team members need to know how each of their individual jobs fit into a successful mission. If team members do not understand how the result of their job could compromise mission success then they will not be able to do a good job of identifying risks.

Understanding mission success also involves the creation of measurable success criteria for both full and minimum success. Understanding science requirements and success criteria are necessary for assessing the ultimate consequences of risks.

Defining acceptable risk to mission success is also important although more difficult. Sometimes computing probability of full and minimum mission success is used. Usually defining the extent of assurance activities from a range of mission classifications helps in this regard. Missions can be classified according to a range from A, B, C, D, with class D allowing a lower level of assurance activities, while class A provides the most detailed and rigorous activities. The mission classifications provide a guide for the extent of assurance activities.[5] These classifications are not meant to indicate rigid boundaries but can be used as a guide when defining activities consistent with a project's acceptable risk.

2. Understanding How systems work. Quoting from the NASA Systems Engineering Handbook SP-6105, "The objective of systems engineering is to see to it that the system is designed, built, and operated so that it accomplishes its purpose in the most cost-effective way possible, considering performance, cost, schedule and risk."[6] The project team needs to expend energy and resources to achieve this objective.

One of the Systems Engineering functions is to plan out activities over the course of the project life cycle in a logical manner to minimize the chance of designing in a problem or miss recognizing one. Figure 4 depicts the classical NASA project life cycle along with a set of curves that indicate many options are available at a low cost early in the life cycle while few options remain near the end at significantly higher cost.

The lifecycle encourages a logical, robust and methodical approach, a "crawl before you walk and walk before you run" sequence for efficient development. Development needs to proceed in the proper order, first you need to choose the "right system" before you proceed to design and build the "system right." Out of sequence activities invariably end up with "do overs" or non-optimum systems and designs.

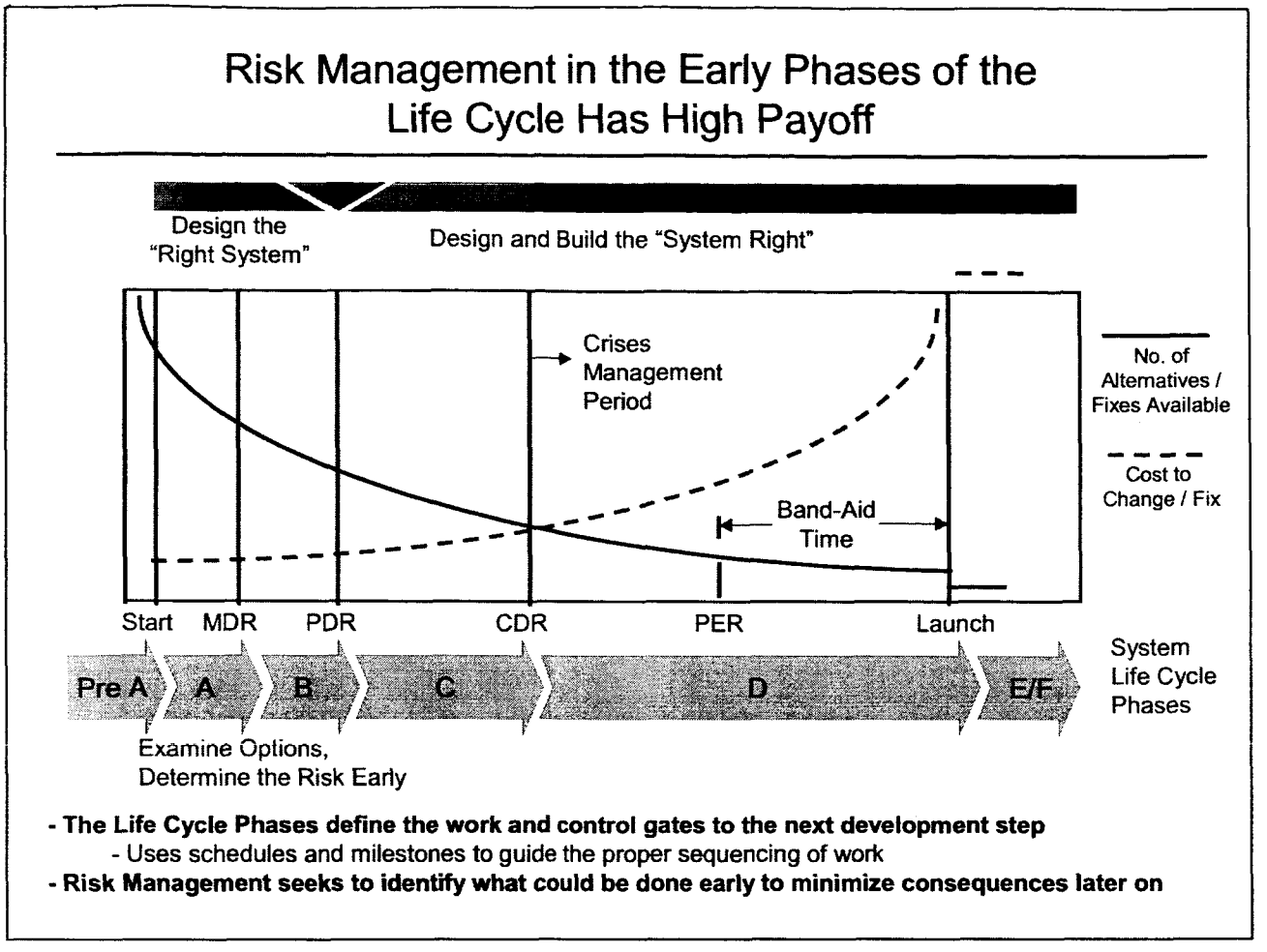

Figure 4 Systems Engineering Lifecycle and Early Risk Identification

Systems engineering guides the life cycle process by logically grouping activities together with milestone reviews. Risk management seeks to identify what should be done early in order to minimize the consequence of a problem later on. Successful teams recognize the value of this proven approach to system development and will expend energy to follow it. These teams realize that those who do not learn from the mistakes of the past, as captured in the proven systems engineering lifecycle, might find that they are destined to repeat those mistakes.

Practical systems engineering and risk management techniques define what should be done to prepare a spacecraft and/or ground system for flight. The techniques need to cover what should be done to efficiently and adequately guide the project towards launch readiness as well as defining the effort planed to uncover potential flaws.

Teams implementing complex aerospace systems need to follow basic universal and non-changing techniques, formulas or principles that form the foundation for successful missions. These principles are documented in handbooks, guidelines, best practices, lessons learned and standards. Without documentation there is a good chance that mistakes of the past will be repeated. Teams and their leaders need to know where these fundamental principles are recorded so they can be accessed.

Multi-layered defenses against human error are naturally included in the lifecycle. The defenses include 1.) sound design rules and principles along with high value reliability analysis that seek to identify a system's weak links, 2.) reviews, 3.) inspections, and 4.) tests. Figure 5 shows a multilayered net with a layer representing each of the major defenses against human error.

Approaches need to be chosen to balance cost and schedule resources while maximizing the value of seeking out what can go wrong. These techniques form the basic principles behind the "management" part of risk management, deciding when and where to expend resources in order to defend against Murphy's Law and Human Error.

The multilayered defenses against human error are described below. Note that it is presumed flaws will exist and that it is the purpose of the multilayered defense to find them.

a. Design Principles. Best practices, lessons learned and sound engineering processes and standards are key to designing complex systems. To avoid repeating the mistakes of the past and learning from them, the best practices need to be captured and followed.

b. Reviews. Allow the input from peers and subject matter experts in order to maximize from the knowledge and experience of others who have solved similar problems

c. Inspection. Looking at the actual system as produced is critical. This function ranges from looking at systems from a workmanship standpoint as well as from a functional standpoint. Was the system built as intended as opposed as it was described on the drawings.

d. Test. Testing forms the best line of defense especially if the item is tested as it will be flown. Exposing the system to a flight like environment using flight like operational scenarios is the ultimate test of the design, assumptions, and any supporting analysis. The purpose of testing is to find any latent flaws.

Answering flight readiness assessment questions, "Why is the mission ready for flight" with a preponderance of positive supporting evidence is the ideal response. Assessing readiness through the absence of negatives, "It has never failed before" might serve as a warning sign that teams and organizations might not have spent enough energy expecting the unexpected. They may have turned off their risk management and systems engineering thinking caps opening the opportunity for Murphy's Law to ruin the day.[7]

3. How systems fail. We require an inquiring mind and curiosity to make the unknowns known and to make what is uncertain more certain.[8]

Reliability Analyses provide structured techniques that seek to answer "What can go wrong" and "What if" questions and also allow the investigation of alternatives that reduce mission performance risk.[8] One of the challenges has been fitting the analysis into the mainstream project life cycle and then communicating the

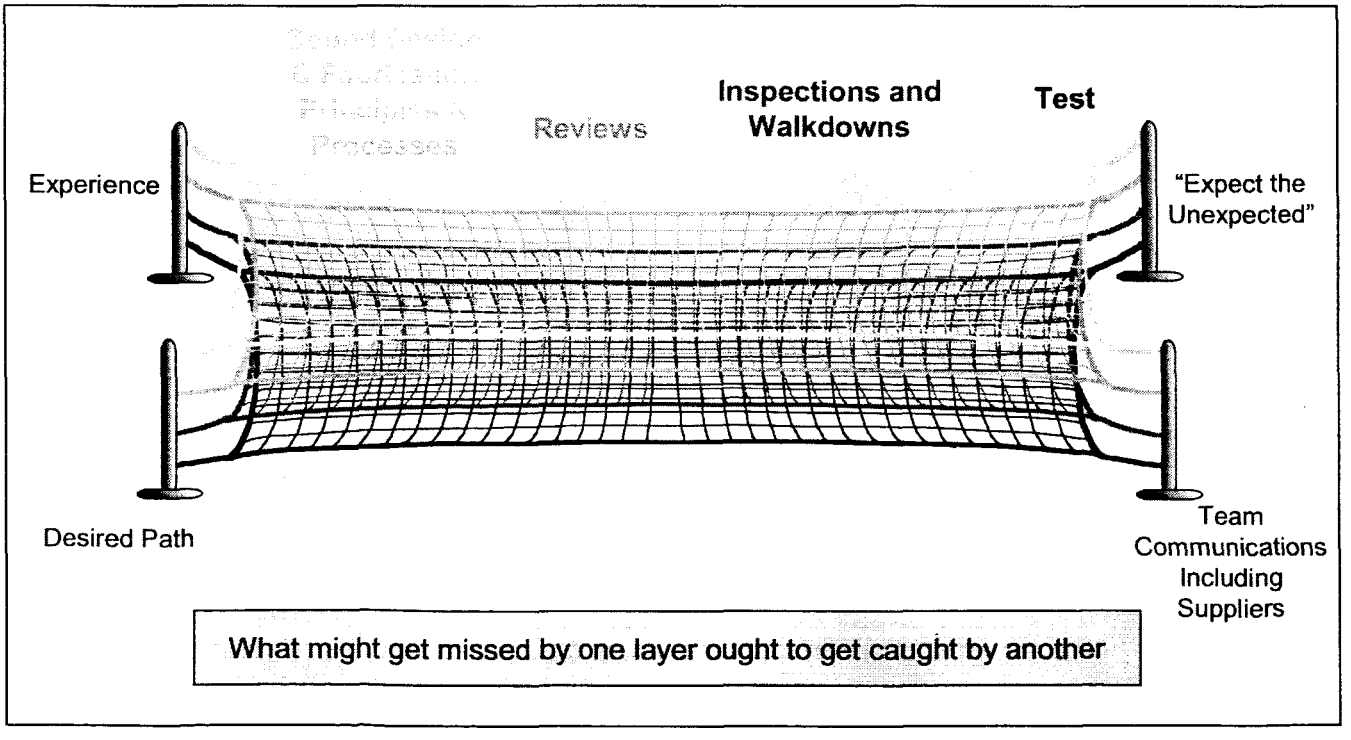

Figure 5 Multilayered Defenses Against Human Error

results of the reliability analysis to the team. One technique that has been used successfully on some projects is a Fault Logic Diagram or an Integrated Logic Diagram[9]

Figure 6 shows the elements of a Fault Logic Diagram that provide a mechanism to summarize, visualize, and review threats to mission success[4]. The diagram integrates threats identified through various Reliability Analyses (Fault Tree Analysis, Failure Modes and Effects Analysis, Reliability Block Diagrams,) into a graphic similar to a Fault Tree.

The diagram provides the users a technique to graphically discriminate between events that are single point failures (red box), that result in graceful degradation (yellow box), or have a minimal mission effect (green box). In this way it helps identify what is important.

The diagram also can be used to identify the controls necessary to prevent or change the outcome of problems (Constraints / Mission Rules, Contingency Procedures, and Fault Protection Algorithms)

One benefit of the Fault Logic Diagram is its ability to collect and summarize information within cost and schedule constrained "medium" to "small" sized missions

It also helps with integrating reliability analysis into the mainstream project life cycle by including software and operator induced initiating events and by including critical contingency procedures and onboard fault detection and correction capabilities. It is important for the team to realize that risk management and reliability analyses are not something done by "others" in a back room somewhere. The diagram shows that the reliability analyses are tightly coupled with mission performance risk management and the controls that are put in place.

Tight budgets and schedule constraints can combine to apply pressure on teams to "get on with it", get ready for launch, at the expense of the rigor and discipline necessary to identify and correct potential problems. When teams answer flight readiness assessment questions with phrases such as "It has never failed before" or

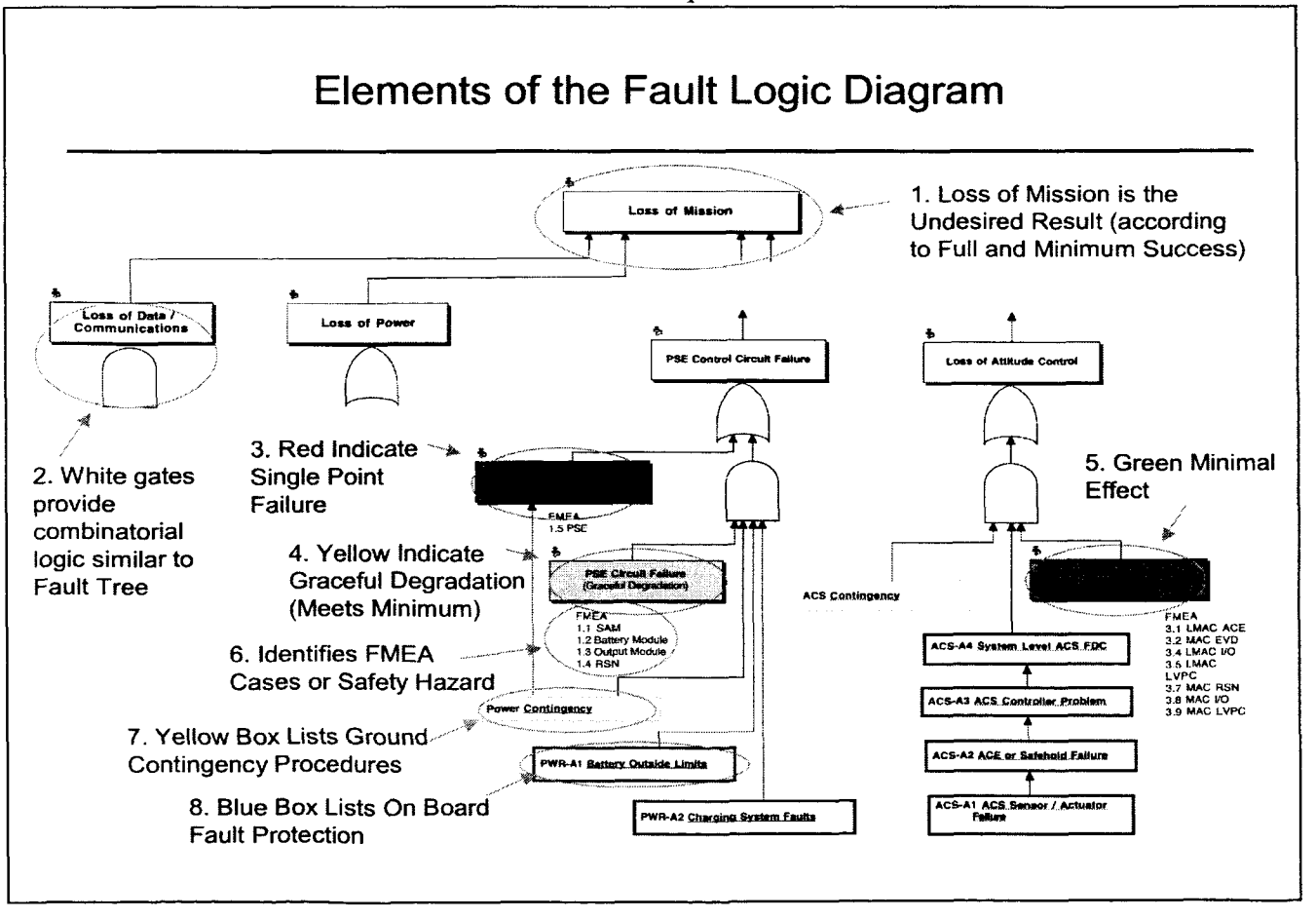

Figure 6 Fault Logic Diagram Elements

"Better is the enemy of good enough" or "I have never worried about this before" or "This is heritage, has flown before, what could possibly go wrong" provides a warning that the necessary rigor and discipline might have been diluted and the effort necessary for a successful mission might have been defocused.

Sound risk management and systems engineering principles ask "What can go wrong" in spite of past success and the absence of failures. There needs to be curiosity amongst team members who need to recognize that a past success may not prove margins going forward. There maybe differences in the application, the environment, or how the system elements were produced that has changed. An improper reliance on "heritage" has been a recurring theme in failure reports that span decades.[10,11] Systems work the way they are built, not necessarily the way they were intended to work. This is a painful lesson to "relearn."

4. What we need to know and learn.

It is important to look for the unknowns and to recognize when you have found one. However it takes experience to know where to look and when you have found something important.

A key characteristic of long lasting successful groups is their expenditure of energy necessary for the constant learning of their personnel as they advance to positions of more responsibility. Yes the best way to learn is by doing. However, life is too short to learn by repeating the mistakes of the past. So leaders need to encourage curiosity into what was done before, how it was done, why it was done, who did it, and where the results are recorded. Typical methods to record what ought to be done include policy, standards, best practice guides, and training materials.

Groups are not static. New people join and they need to learn, people move on to other jobs and may take important knowledge with them. If appropriate effort is put into keeping handbooks, best practices, guidelines and standards current and up to date, then teams at least have the opportunity to learn by following these guides.

If teams want to improve or change while not risking a repeat of a past mistake, they must not throw established procedures out without understanding what they are meant to accomplish, or said differently "Don't throw the baby out with the bath water."[12]

Summary

Risk management techniques are most effective when they are promoted by the project team leader and adopted by the entire team including Systems Engineering, Mission Assurance, Project Management staff, as well as the engineers and technicians that design, produce and operate the system. The whole team adopts risk management as a normal course of doing business and not a separate detached discipline. When the team has a healthy respect for Murphy's Law and a sense of curiosity for how things should work, how they can fail, and what they need to know to make good decisions, they are well on this way to defending against Murphy's Law and mission ending failures.

References:

1. Bay, M., *The Microwave Anisotropy Probe's (MAP) Reliability And Risk Management Program*, (Risk Management 2002 Symposium), May 21, 2002
2. Collins, M, *Carrying the Fire*, (First Cooper Square, 2001), p 195 ("Beyond fallible machines lurked even more fallible humans. There were so many ways in which we could screw up, so many possibilities for error...") (*This book provides an astronaut's perspective of the constant "What happens if" questioning forming the basis of risk management during the trailblazing 1960s*)
3. Kranz, Gene, *Failure Is Not An Option*, (Berkley2000), p 29 ("having the experience to anticipate what *could* happen rather than just reacting to what *was* happening at the moment") (*This book provides excellent insight into risk management thinking processes.)*
4. Bay, M., *The Power of an Integrated Logic Diagram for Risk Management*, (Risk Management Colloquium IV Sept 3-5, 2003)
5. NASA, *NASA Systems Engineering Handbook, SP-6105*, 1995, Appendix B3
6. NASA, *NASA Systems Engineering Handbook, SP-6105*, 1995, p4 Section 2.3
7. Kraft, C., *Flight, My Life in Mission Control*, (Dutton, 2001), p 98 ("If somebody says that something never happens, be prepared because it probably will"), (*This book provides good insight into the degree that the early manned spaceflight era focused on expecting the unexpected and not taking success for granted. They focused on making the unknowns known and being prepared should one surface*)

8. Kraft, C., *Flight, My Life in Mission Control*, 2001, p 81 ("What systems can cause a catastrophic failure, and what measurements can forecast that failure?")
9. Kraft, C., *Flight, My Life in Mission Control*, (Dutton, 2001), p 100 ("What about the unknown unknowns?", "What if? What if this happens? What if that breaks? What if this happens and that breaks at the same time?")
10. NASA, *Report of the SEASAT Failure Review Board*, December 21, 1978
11. NASA, *Contour Mishap Investigation Report*, May 31, 2003
12. Lemonick, Michael D., *Echo of the Big Bang,* (Princeton University Press, 2003), p-127 ("Don't do things a certain way just because NASA has always done them that way. But Don't throw procedures out without understanding what they're meant to accomplish"), (*MAP is an example of a cost and schedule constrained mission that actively engaged in risk management to help guide the expenditure of resources)*